

CLAIMS:

1. System for copy protection of recorded information, comprising an information carrier comprising a medium mark representing a first bitpattern (x), a recorder for recording the information on the information carrier and a player for reproducing the recorded information from the information carrier, characterized in that the recorded information comprises a watermark representing a second bitpattern (y), which second bitpattern has a predefined relationship to the first bitpattern, and in that the recorder comprises encoder means (23) for embedding the watermark in the information and generator means (25) for generating the second bitpattern according to the predefined relationship between the first and the second bitpattern, and in that the player comprises verification means (29) for verifying the relationship between the second bitpattern and the first bitpattern.

2. System as claimed in claim 1, characterized in that the relationship comprises a cryptographic one-way function.

3. System as claimed in claim 2, characterized in that the second bitpattern (y) is generated by applying a one-way function to the first bitpattern (x).

4. System as claimed in claim 1, 2 or 3, characterized in that the second bitpattern identifies the encoder means.

5. Recorder for use in the system of claim 1, 2, 3 or 4 for recording information on an information carrier comprising a medium mark representing a first bitpattern (x), characterized in that the recorder comprises encoder means (42) for embedding a watermark in the information, the watermark representing a second bitpattern (y), and generator means (43) for generating the second bitpattern according to a predefined relationship between the first and the second bitpattern.

6. Recorder as claimed in claim 5, characterized in that the recorder comprises marking means (46) for creating the medium mark on the information carrier and in that the generator means comprise means (44) for generating the first bitpattern from a seed (u) according to a further predefined relationship.

7. Recorder as claimed in claim 5 or 6, characterized in that the generator means (43) are arranged for generating the first bitpattern (x) by combining a first part (x₀)

Sub
0901344-013636
363610-175209

16.01.1998

represented by a prepressed mark on a recordable information carrier and a second part (x_2) generated from the seed (u).

8. Recorder as claimed in claim 6 or 7, characterized in that the further predefined relationship comprises a cryptographic one-way function.

5 9. Information carrier for use in the system of claim 1, 2, 3 or 4, the information carrier (51) comprising recorded information and a medium mark (50) representing a first bitpattern (x), characterized in that the recorded information comprises a watermark representing a second bitpattern (y), which second bitpattern has a predefined relationship to the first bitpattern.

10 10. Information carrier as claimed in claim 9, characterized in that the first bitpattern comprises a first part (x_c) identifying a source of the information carrier, and a second part (x_r) identifying the recorded information.

11. Player for use in the system of claim 1, 2, 3 or 4 for reproducing information from an information carrier (51) and comprising means (50) for detecting a medium mark representing a first bitpattern (x), characterized in that the player comprises watermark read means (55) for detecting a second bitpattern (y) represented by a watermark in the recorded information, and in that the player comprises verification means (53,54) for verifying a predefined relationship between the second bitpattern and the first bitpattern.

12. Player as claimed in claim 1, characterized in that the verification means
20 comprise a cryptographic one-way function (53).

13. Player as claimed in claim 12, characterized in that the verifications means are arranged for generating a verification pattern (y') by applying a one-way function to the first bitpattern (x) and comprises means (54) for comparing the verification pattern (y') and the second bitpattern (y).

[illegible]
$$a^2$$

Add 7

~~add~~

Q12